

## NETWORK SECURITY ARCHITECTURE SYSTEM UTILIZING SEALS

Daniel F. Zucker

### 5 ABSTRACT

5       An efficient multicast key management is achieved  
by using seals. A security server generates a seal.  
In one embodiment, the seal contains a key. In another  
embodiment, the seal contains information for  
10   generating a key. An application server requests the  
seal from the security server and broadcasts the seal  
to a plurality of recipients. A recipient wishing to  
encrypt or decrypt a data stream transmits the received  
seal to the security server to be opened. If the  
15   recipient is authorized, the security server transmits  
a permit to the authorized recipient. In one  
embodiment, the recipient generates a key from the  
permit. In another embodiment, the permit is the key.  
If the recipient is a sender, the recipient encrypts  
20   data using the key and broadcasts the same encrypted  
data stream to all receivers. If the recipient is a  
receiver, the recipient decrypts an encrypted data  
stream using the key. In one embodiment, a seal with a  
corresponding offset value is sent periodically in a  
25   data stream. In another embodiment, multiple instances  
of identical seals are opened only once. In yet  
another embodiment, a seal is appended to each datagram  
packet. In a further embodiment, a seal is appended to  
any data stream.

30